

Standards	Sections	Implementation Specifications (R)=Required, (A)=Addressable
Security Awareness and Training .....	164.308(a)(5)	Access Authorization (A) Access Establishment and Modification (A) Security Reminders (A) Protection from Malicious Software (A) Log-in Monitoring (A) Password Management (A) Response and Reporting (R) Data Backup Plan (R)
Security Incident Procedures .....	164.308(a)(6)	Disaster Recovery Plan (R) Emergency Mode Operation Plan (R) Testing and Revision Procedure (A)
Contingency Plan .....	164.308(a)(7)	Applications and Data Criticality Analysis (A) (R)
Evaluation .....	164.308(a)(8)	Written Contract or Other Arrangement (R)
Business Associate Contracts and Other Arrangement.	164.308(b)(1)	
<b>Physical Safeguards</b>		
Facility Access Controls .....	164.310(a)(1)	Contingency Operations (A) Facility Security Plan (A) Access Control and Validation Procedures (A) Maintenance Records (A)
Workstation Use .....	164.310(b)	(R)
Workstation Security .....	164.310(c)	(R)
Device and Media Controls .....	164.310(d)(1)	Disposal (R) Media Re-use (R) Accountability (A) Data Backup and Storage (A)
<b>Technical Safeguards</b> (see § 164.312)		
Access Control .....	164.312(a)(1)	Unique User Identification (R) Emergency Access Procedure (R) Automatic Logoff (A) Encryption and Decryption (A)
Audit Controls .....	164.312(b)	(R)
Integrity .....	164.312(c)(1)	Mechanism to Authenticate Electronic Protected Health Information (A)
Person or Entity Authentication .....	164.312(d)	(R)
Transmission Security .....	164.312(e)(1)	Integrity Controls (A) Encryption (A)

**Subpart D—Notification in the Case of Breach of Unsecured Protected Health Information**

SOURCE: 74 FR 42767, Aug. 24, 2009, unless otherwise noted.

**§ 164.400 Applicability.**

The requirements of this subpart shall apply with respect to breaches of protected health information occurring on or after September 23, 2009.

**§ 164.402 Definitions.**

As used in this subpart, the following terms have the following meanings:

*Breach* means the acquisition, access, use, or disclosure of protected health information in a manner not permitted under subpart E of this part which

compromises the security or privacy of the protected health information.

(1)(i) For purposes of this definition, *compromises the security or privacy of the protected health information* means poses a significant risk of financial, reputational, or other harm to the individual.

(ii) A use or disclosure of protected health information that does not include the identifiers listed at § 164.514(e)(2), date of birth, and zip code does not compromise the security or privacy of the protected health information.

(2) Breach excludes:

(i) Any unintentional acquisition, access, or use of protected health information by a workforce member or person acting under the authority of a covered entity or a business associate, if such acquisition, access, or use was

## § 164.404

## 45 CFR Subtitle A (10–1–12 Edition)

made in good faith and within the scope of authority and does not result in further use or disclosure in a manner not permitted under subpart E of this part.

(ii) Any inadvertent disclosure by a person who is authorized to access protected health information at a covered entity or business associate to another person authorized to access protected health information at the same covered entity or business associate, or organized health care arrangement in which the covered entity participates, and the information received as a result of such disclosure is not further used or disclosed in a manner not permitted under subpart E of this part.

(iii) A disclosure of protected health information where a covered entity or business associate has a good faith belief that an unauthorized person to whom the disclosure was made would not reasonably have been able to retain such information.

*Unsecured protected health information* means protected health information that is not rendered unusable, unreadable, or indecipherable to unauthorized individuals through the use of a technology or methodology specified by the Secretary in the guidance issued under section 13402(h)(2) of Public Law 111–5 on the HHS Web site.

### § 164.404 Notification to individuals.

(a) *Standard*—(1) *General rule*. A covered entity shall, following the discovery of a breach of unsecured protected health information, notify each individual whose unsecured protected health information has been, or is reasonably believed by the covered entity to have been, accessed, acquired, used, or disclosed as a result of such breach.

(2) *Breaches treated as discovered*. For purposes of paragraph (a)(1) of this section, §§ 164.406(a), and 164.408(a), a breach shall be treated as discovered by a covered entity as of the first day on which such breach is known to the covered entity, or, by exercising reasonable diligence would have been known to the covered entity. A covered entity shall be deemed to have knowledge of a breach if such breach is known, or by exercising reasonable diligence would have been known, to any person, other than the person com-

mitting the breach, who is a workforce member or agent of the covered entity (determined in accordance with the federal common law of agency).

(b) *Implementation specification: Timeliness of notification*. Except as provided in § 164.412, a covered entity shall provide the notification required by paragraph (a) of this section without unreasonable delay and in no case later than 60 calendar days after discovery of a breach.

(c) *Implementation specifications: Content of notification*—(1) *Elements*. The notification required by paragraph (a) of this section shall include, to the extent possible:

(A) A brief description of what happened, including the date of the breach and the date of the discovery of the breach, if known;

(B) A description of the types of unsecured protected health information that were involved in the breach (such as whether full name, social security number, date of birth, home address, account number, diagnosis, disability code, or other types of information were involved);

(C) Any steps individuals should take to protect themselves from potential harm resulting from the breach;

(D) A brief description of what the covered entity involved is doing to investigate the breach, to mitigate harm to individuals, and to protect against any further breaches; and

(E) Contact procedures for individuals to ask questions or learn additional information, which shall include a toll-free telephone number, an e-mail address, Web site, or postal address.

(2) *Plain language requirement*. The notification required by paragraph (a) of this section shall be written in plain language.

(d) *Implementation specifications: Methods of individual notification*. The notification required by paragraph (a) of this section shall be provided in the following form:

(1) *Written notice*. (i) Written notification by first-class mail to the individual at the last known address of the individual or, if the individual agrees to electronic notice and such agreement has not been withdrawn, by electronic mail. The notification may be